

in working order so that no unsafe conditions exist.

(e) *Procedures.* A launch operator must conduct each launch processing or post-launch operation involving a public hazard or a launch location hazard pursuant to written procedures that incorporate the hazard controls identified by a launch operator's ground safety analysis and as required by this subpart. The person designated in § 417.103(b)(2) must approve the procedures. A launch operator must maintain an "as-run" copy of each procedure. The "as-run" procedure copy must include changes, start and stop dates, and times that each procedure was performed and observations made during the operations.

(f) *Hazardous materials.* A launch operator must establish procedures for the receipt, storage, handling, use, and disposal of hazardous materials, including toxic substances and sources of ionizing radiation. A launch operator must establish procedures for responding to hazardous material emergencies and protecting the public that complies with the accident investigation plan as defined in § 417.111(h)(2). These procedures must include:

- (1) Identification of each hazard and its effects;
- (2) Actions to be taken in response to release of a hazardous material;
- (3) Identification of protective gear and other safety equipment that must be available in order to respond to a release;
- (4) Evacuation and rescue procedures;
- (5) Chain of command; and
- (6) Communication both on-site and off-site to surrounding communities and local authorities.

(g) *Toxic release hazard notifications and evacuations.* A launch operator must perform a toxic release hazard analysis for launch processing performed at the launch site that satisfies section I417.7 of this part. A launch operator must apply toxic plume modeling techniques that satisfy section I417.7 of this part and ensure that notifications and evacuations are accomplished to protect the public from potential toxic release.

#### § 417.409 System hazard controls.

(a) *General.* A launch operator must establish and maintain hazard controls for each system that presents a public hazard as identified by the ground safety analysis and satisfy the requirements of this section. A launch operator must:

(1) Ensure a system be at least single fault tolerant to creating a public hazard unless other hazard control criteria are specified for the system by the requirements of this part. A system capable of creating a catastrophic public hazard must be at least dual fault tolerant. Dual fault tolerant system hazard controls include: Switches, valves, or similar components that prevent an unwanted transfer or release of energy or hazardous materials;

(2) Ensure each hazard control used to provide fault tolerance is independent from other hazard controls so that no single action or event can remove more than one inhibit. A launch operator must prevent inadvertent activation of hazard control devices such as switches and valves;

(3) Provide at least two fully redundant safety devices if a safety device must function in order to control a public hazard. A single action or event must not be capable of disabling both safety devices; and

(4) Ensure computing systems and software used to control a public hazard satisfy the requirements of § 417.123.

(b) *Structures and material handling equipment.* A launch operator must ensure safety factors applied in the design of a structure or material handling equipment account for static and dynamic loads, environmental stresses, expected wear, and duty cycles. A launch operator must:

(1) Inspect structures and material handling equipment to verify workmanship, proper operations, and maintenance;

(2) Prepare plans to ensure proper operations and maintenance of structures and material handling equipment;

(3) Assess structures and material handling equipment for potential single point failure;

(4) Eliminate single point failures from structures and material handling equipment or subject the structures

and material handling equipment to specific inspection and testing to ensure proper operation. Single point failure welds must undergo both surface and volumetric non-destructive inspection to verify that no rejectable discontinuities exist;

(5) Establish other non-destructive inspection techniques if a volumetric inspection cannot be performed. A launch operator, in such a case, must demonstrate through the licensing process that the inspection processes used accurately verify the absence of rejectable discontinuities; and

(6) Ensure qualified and certified personnel, as defined in §417.105, conduct the inspections.

(c) *Pressure vessels and pressurized systems.* A launch operator must apply the following hazard controls to a pressurized flight or ground pressure vessel, component, or systems:

(1) Qualified and certified personnel, as defined in §417.105, must test each pressure vessel, component, or system upon installation and before being placed into service, and periodically inspect to ensure that no rejectable discontinuities exist;

(2) Safety factors applied in the design of a pressure vessel, component, or system must account for static and dynamic loads, environmental stresses, and expected wear;

(3) Pressurized system flow-paths, except for pressure relief and emergency venting, must be single fault tolerant to causing pressure ruptures and material releases during launch processing; and

(4) Provide pressure relief and emergency venting capability to protect against pressure ruptures. Pressure relief devices must provide the flow rate necessary to prevent a rupture in the event a pressure vessel is exposed to fire.

(d) *Electrical and mechanical systems.* A launch operator must apply the following hazard controls to electrical or mechanical systems that can release electrical or mechanical energy during launch processing:

(1) A launch operator must ensure electrical and mechanical systems, including systems that generate ionizing or non-ionizing radiation, are single

fault tolerant to providing or releasing electrical or mechanical energy;

(2) In areas where flammable material exists, a launch operator must ensure electrical systems and equipment are hermetically sealed, explosion proof, intrinsically safe, purged, or otherwise designed so as not to provide an ignition source. A launch operator must assess each electrical system as a possible source of thermal energy and ensure that the electrical system can not act as an ignition source; and

(3) A launch operator must prevent unintentionally conducted or radiated energy due to possible bent pins in a connector, a mismatched connector, shorted wires, or unshielded wires within electrical power and signal circuits that interface with hazardous subsystems.

(e) *Propulsion systems.* A propulsion system must be dual fault tolerant to inadvertently becoming propulsive. Propulsion systems must be single fault tolerant to inadvertent mixing of fuel and oxidizer. Each material in a propulsion system must be compatible with other materials that may contact the propulsion system during launch processing including materials used to assemble and clean the system. A launch operator must use engineering controls, including procedures, to prevent connecting incompatible systems. A launch operator must comply with §417.417 for hazard controls applicable to propellants and explosives.

(f) *Ordnance systems.* An ordnance system must be at least single fault tolerant to prevent a hazard caused by inadvertent actuation of the ordnance system. A launch operator must comply with §417.417 for hazard controls applicable to ordnance. In addition, an ordnance system must satisfy the following requirements;

(1) A launch operator must ensure ordnance electrical connections are disconnected until final preparations for flight;

(2) An ordnance system must provide for safing and arming of the ordnance. An electrically initiated ordnance system must include ordnance initiation devices and arming devices, also referred to as safe and arm devices, that provide a removable and replaceable mechanical barrier or other positive

means of interrupting power to each ordnance firing circuit to prevent inadvertent initiation of ordnance. A mechanical safe and arm device must have a safing pin that locks the mechanical barrier in a safe position. A mechanical actuated ordnance device must also have a safing pin that prevents mechanical movement within the device. A launch operator must comply with section D417.13 of this part for specific safing and arming requirements for a flight termination system;

(3) Protect ordnance systems from stray energy through grounding, bonding, and shielding; and

(4) Current limit any monitoring or test circuitry that interfaces with an ordnance system to protect against inadvertent initiation of ordnance. Equipment used to measure bridgewire resistance on electro-explosive devices must be special purpose ordnance system instrumentation with features that limit current.

**§417.411 Safety clear zones for hazardous operations.**

(a) A launch operator must define a safety clear zone that confines the adverse effects of each operation involving a public hazard or launch location hazard. A launch operator's safety clear zones must satisfy the following:

(1) A launch operator must establish a safety clear zone that accounts for the potential blast, fragment, fire or heat, toxic and other hazardous energy or material potential of the associated systems and operations. A launch operator must base a safety clear zone on the following criteria:

(i) For a possible explosive event, base a safety clear zone on the worst case event, regardless of the fault tolerance of the system;

(ii) For a possible toxic event, base a safety clear zone on the worst case event. A launch operator must have procedures in place to maintain public safety in the event toxic releases reach beyond the safety clear zone; and

(iii) For a material handling operation, base a safety clear zone on a worst case event for that operation.

(2) A launch operator must establish a safety clear zone when the launch vehicle is in a launch command configuration with the flight safety systems

fully operational and on internal power.

(b) A launch operator must establish restrictions that prohibit public access to a safety clear zone during a hazardous operation. A safety clear zone may extend to areas beyond the launch location boundaries if local agreements provide for restricting public access to such areas and a launch operator verifies that the safety clear zone is clear of the public during the hazardous operation.

(c) A launch operator's procedures must verify that the public is outside of a safety clear zone prior to a launch operator beginning a hazardous operation.

(d) A launch operator must control a safety clear zone to ensure no public access during the hazardous operation. Safety clear zone controls include:

(1) Use of security guards and equipment;

(2) Physical barriers; and

(3) Warning signs, and other types of warning devices.

**§417.413 Hazard areas.**

(a) *General.* A launch operator must define a hazard area that confines the adverse effects of a hardware system should an event occur that presents a public hazard or launch location hazard. A launch operator must prohibit public access to the hazard area whenever a hazard is present unless the requirements for public access of paragraph (b) of this section are met.

(b) *Public access.* A launch operator must establish a process for authorizing public access if visitors or members of the public must have access to a launch operator's facility or launch location. The process must ensure that each member of the public is briefed on the hazards within the facility and related safety warnings, procedures, and rules that provide protection, or a launch operator must ensure that each member of the public is accompanied by a knowledgeable escort.

(c) *Hazard controls during public access.* A launch operator must establish procedural controls that prevent hazardous operations from taking place while members of the public have access to the launch location and must verify that system hazard controls are